ESG SHOWCASE

ZeroNorth: Automating and Orchestrating Application Security Across the SDLC, from Code Commit through Build to Deployment

Date: February 2021 **Author:** Dave Gruber, Senior ESG Analyst

ABSTRACT:

- Most organizations employ multiple software development teams, while many utilize complex supply chains that depend heavily on software-driven components. This fragmented development world makes it difficult for security teams to gain control over software testing and even more difficult to assess and mitigate risk throughout their application portfolios.
- Security teams and risk managers need to understand risk/vulnerabilities across the software development lifecycle, from code commit through build to deployment. This understanding allows teams to prioritize risk mitigation based on application criticality and risk assessment.
- With the continuing complexity of application security, there is a need for a single orchestration platform that can simplify the process of managing scanning tools and technologies. New innovations by vendors like ZeroNorth enable security teams to scale up their application security initiatives, while introducing new tools without disruption to their application development and DevOps environments.

Overview

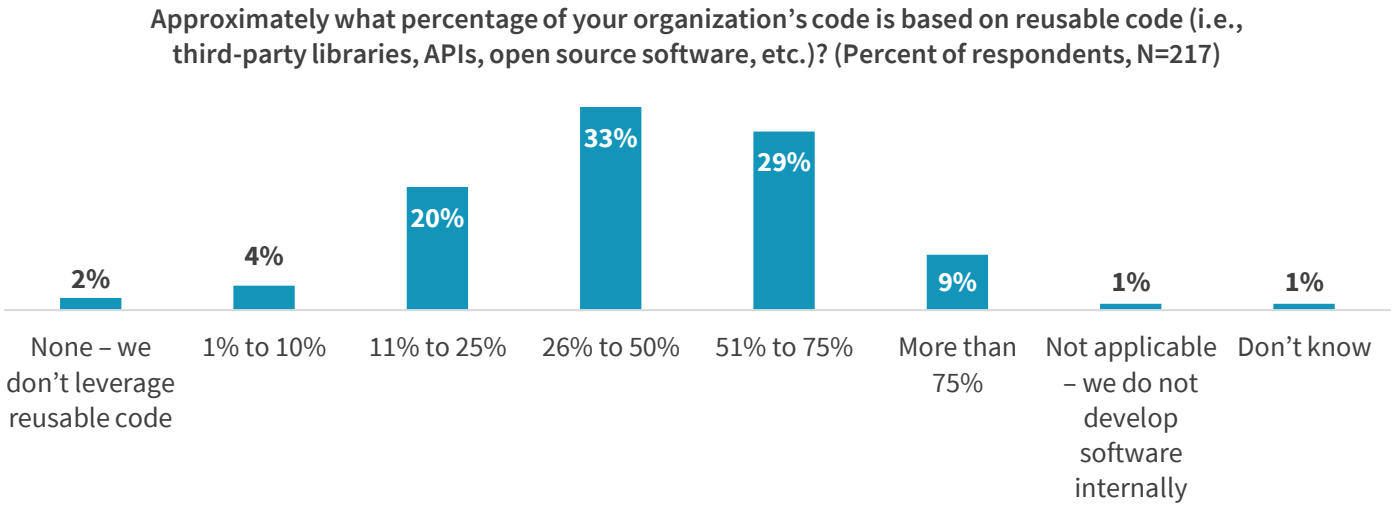
Today's enterprises depend on their software development teams to compete effectively in our modern, technology-driven economy. With the pace of application development at an all-time high, as businesses leverage rapid development cycles and DevOps deployment models, they depend on the introduction of new features to differentiate their offerings.

Most organizations employ multiple software development teams, while many utilize complex supply chains that depend heavily on software-driven components. This fragmented development world makes it difficult for security teams to gain control over software testing and even more difficult to assess and mitigate risk throughout their application portfolios.

Even with internal security training, heavy dependence on code reuse means that apps are at risk. Code reuse is core to modern application development, with respondents reporting that 71% of applications are built using more than 25% reusable code. Yet with less than 50% of apps utilizing automated AppSec testing tools, organizations are exposed.[1]

[1] Source: ESG Master Survey Results, *Application and Email Security Survey*, September 2019.

Figure 1. Code Reuse Is Core to Application Development



Source: Enterprise Strategy Group

Today's development organizations are leveraging many individual tools to discover and remediate vulnerabilities. While application security and vulnerability management vendors consolidate tool offerings in an effort to integrate the testing and vulnerability assessment process, few organizations depend solely on a single vendor to supply all of their testing tools.

Many organizations instead utilize a best-of-breed strategy, employing SCA, SAST, artifact/registry scanning, container scanning, pen testing, network scanning, and vulnerability scanning tools from multiple vendors. Because most of these tools are unable to share information, this strategy makes it difficult for security teams to broadly assess overall risk associated with their application portfolio. Further, all applications are not equal in terms of their importance to an organization. Mission-critical applications require more visibility and faster assessment and remediation of identified risks.

This paper will explore these challenges and recommend an approach to help organizations more effectively secure their application portfolios through the use of application security scanning and testing orchestration.

Six Application Security Management Challenges

Security leaders face multiple challenges as their organizations move towards, or through, their digital transformations. Risk assessment prioritization is a core component of running an effective security program. However, assessing and prioritizing risk associated with applications is a challenging task for most security leaders.

1. Challenge: Gaining Software Risk Visibility and Assurance

When it comes to managing application security risk, organizations are often flying blind. They lack comprehensive, continuous, and accurate visibility into where their risks lie and how their business might be impacted. Without visibility, it's impossible to prioritize and manage IT risk.

IT teams are struggling to keep up with configuration, patching, and compliance management.

Existing ad hoc and siloed approaches are labor-intensive and expensive, resulting in limited deployments and incomplete visibility. While usage of AppSec tools has increased steadily in the past five years, 60% of organizations are still only leveraging AppSec testing tools on 50% or less of their apps.[2]

And without a closed-loop process, risk managers have no means to validate remediation.

2. Challenge: Scaling an Application Management Risk Framework

With each testing tool depending on its own policy and risk framework, security teams are tasked with aligning overall organizational security policies across the portfolio of testing tools.

With each tool employing its own policy model, it is often difficult for organizations to consistently implement policies across the many tools. Rolling out policy changes can be resource- and time-intensive, slowing the security team's ability to act fast when changes are required.

3. Challenge: Securing DevOps

DevOps models have revolutionized the development and delivery of software, enabling organizations to transform their organizations into the digital era. These models provide greater levels of agility, accelerated time to market, and a better customer experience.

While DevOps models deliver competitive advantage for most companies, they also have introduced a new level of risk, often shedding needed security controls in the process. Without an integrated security and risk management model for DevOps, organizations can be left wide open to cyber-attacks, lost revenue, and a loss of customer trust.

4. Challenge: Automating Application Security Testing

Organizations typically employ multiple testing tools, sometimes ten or more different tools. Each tool has its own interface and APIs, requiring separate integration into the DevOps toolchain. Individual tools also categorize results differently, creating a heavily manual, labor-intensive, and error-prone task to correlate vulnerability data into actionable intelligence.

Because of these complexities, most tools require separate, skilled security resources to manage each tool. With the well-known security skills shortage, organizations struggle to hire the staffing required to run effective application security programs across their entire software portfolios.

5. Challenge: Integrating Fragmented Security Scanning Tools

With companies employing hundreds of software development teams, both internally and through third-party software supply chains, few have standardized on testing tools company-wide, leaving security teams with a fragmented set of tooling that is difficult to integrate, and even more difficult to assess and mitigate overall risk. Between 49% and 63% of organizations report the use of multiple, disparate testing tools ranging from SAST, DAST, IAST, SCA, and other vulnerability scanning tools, with another 25-31% planning on further investment in tooling in the next 12-18 months.[3]

To make matters worse, individual subject matter experts are often required to support and manage individual tools, diverting cybersecurity resources from more critical and strategic priorities while increasing overall costs.

[2] Source: ESG Master Survey Results, *Application and Email Security Survey*, September 2019.
[3] Source: ESG Master Survey Results, *Application and Email Security Survey*, September 2019.

6. Challenge: Ensuring PCI/DSS Compliance

For cybercriminals, credit card data is a gold mine. Left unprotected, hackers do all they can to steal cardholder data. Protecting this information has become a risk and security management priority for banks, credit card companies, and businesses.

To address these challenges, the Payment Card Industry Data Security Standard was created. The PCI DSS consists of 12 high-level requirements for protecting credit card information. All organizations that store, process, or transmit cardholder data—including banks, merchants, processors, and service providers—are required to comply.

PCI DSS Requirement 6: Develop and maintain secure systems and applications

With Requirement 6, the PCI DSS makes clear the importance of application security and vulnerability management with respect to the systems that process, transmit, or store cardholder data. More specifically, PCI DSS requires companies to establish a process for identifying and remediating vulnerabilities. The standard also directs companies to ensure security is incorporated throughout the SDLC.

PCI DSS Requirement 11: Regularly test security systems and processes

As stressed in Requirement 11, vulnerability management is a cornerstone of protecting cardholder data and reducing cyber risk. The standard requires companies to run internal and external network scans, and to employ a methodology for penetration testing.

To address PCI Requirements 6 and 11, companies deploy a range of tools to continuously monitor application security throughout the CI/CD pipeline (e.g., SAST, DAST, SCA). In addition, various threat vulnerability management and penetration testing tools identify threats across infrastructure.

Yet, even with these controls in place, companies lack a complete and actionable view of application and infrastructure risk, creating opportunity for attackers to steal credit card data.

What's Needed: Orchestrated Application Security

To address the complexity of application security testing, organizations need a single orchestration platform that can simplify the process of managing multiple scanning and testing tools and technologies.

The platform needs to provide a consolidated, continuous assessment of application security risk across the SDLC and the entire application portfolio, with the ability to enable risk-based assessment that can focus on prioritized individual business assets. The solution must also be able to assess the effectiveness of individual development teams.

In today's complex deployment environment, the solution must be able to provide a consolidated view of risk to critical business assets, whether on-premises, in the cloud, or deployed as microservices.

The platform needs to span both applications and infrastructure, providing a consolidated, continuous assessment of risk across the SDLC.

As an application security platform, the solution needs to automate the onboarding and management of all application security scanning tools, including identifying scan targets, scheduling scans, and executing scans. It must also provide the ability to consistently test, select, and onboard scanning tools across the software development lifecycle enabling teams to add or remove tools easily, as needed.

In addition to correlating and normalizing scan data, the platform must be able to drive all the tools from a single console, orchestrating the overall process associated with the usage, assessment, and PCI/DSS compliance reporting.

To make this solution operate seamlessly, the platform must easily integrate with all application security, development, and DevOps tools.

Introducing ZeroNorth AppSec Automation & Orchestration Platform

The ZeroNorth AppSec automation and orchestration platform delivers a single pane of glass for managing application security scanning tools, including scheduling scans, correlating scan results, and aligning risk with critical business assets. While automating the operational orchestration of the process, ZeroNorth provides easy-to-understand executive-level views of the security and risk aligned with critical business assets.

As a platform, ZeroNorth provides out-of-the-box connectors that support rapid ingestion of data from the broadest range of scanning tools and developer environments. It also includes integrated open source scanning tools to enable capability comparison and testing and to fill gaps in a scanning portfolio.

By orchestrating the many scanning tools used across the entire software lifecycle, ZeroNorth provides a comprehensive and continuous view of vulnerabilities and risk, ultimately reducing costs associated with managing disparate technologies. This visibility enables security teams to more effectively assess and prioritize risk mitigation activities, leading to improved security and compliance by eliminating fragmented views of vulnerabilities throughout the SDLC.

This orchestration also helps security and risk teams rapidly scale application security, while integrating seamlessly into developer environments to simplify and verify remediation.

The Bigger Truth

Application vulnerability and risk assessment are key components of successful security programs while DevSecOps processes are critical to enabling businesses to compete effectively and securely. With organizations depending on multiple security solutions and vendors to assess and remediate issues, security teams struggle to ensure that critical business applications are secured.

New innovations by vendors like ZeroNorth enable security teams to scale up their application security initiatives while increasing the effectiveness of their efforts. These innovations can further help organizations acquire the flexibility to easily introduce new tools without disrupting their application security frameworks. Organizations that leverage application security scanning and testing tools as part of their software development processes should consider the use of an automation and orchestration platform like ZeroNorth to improve their ability to assess risk, prioritize critical business applications, and gain the flexibility to rapidly onboard new testing solutions to speed development while increasing the effectiveness of their security programs.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188